

THE COMPUTER AND SECURITY

Captain Charles E. Smith, USN
Deputy Director
Residence School
Industrial College of the Armed Forces
Fort Lesley J. McNair
Washington, D.C. 20315

Prepared for Course 617
Survey of Data Processing and Management Information Systems
Spring 1970

Copies Distributed
at the
13th Annual Area Conference
Association of Records Executives and Administrators
Greater Washington, D.C. Chapter

29 April 1970

Twin Bridges Marriott Motor Hotel
Washington, D.C.

The Computer and Security

In the world of business competition there has always been a problem of protecting proprietary information, from a secret recipe for barbecue sauce to the most sophisticated design information for a supersonic aircraft. There are now over 60,000 computers installed in the United States being used in various business and governmental applications(1). Most of these have been manufactured in the past twenty years. How has this relatively sudden adoption of computers changed the security problem? For one thing, it has resulted in a higher concentration of information in a single location. This might appear at first to improve security for it is easier to provide physical security for the limited space of a computer facility than for acres of file cabinets. However there are other aspects to this development which decrease security. The information in the computer system is more organized as well as more concentrated, and therefore is more vulnerable to unauthorized access. Hard copy files can only be lost by theft or physical destruction such as fire. Computer files can be magnetically erased, accidentally or intentionally. This can be caused by a hardware malfunction, software error or improper operating procedure. Systems with remote terminals or that can be accessed through common carriers are always subject to use by unauthorized persons unless proper security measures are taken.

From the evidence available it appears that the introduction of the computer has complicated the security problem. The situation is worsened by the fact that only recently has there been a widespread interest in the problem. All the answers are not yet in. Mr. Van Buelow reported at the 15th Annual Seminar of the American

Society for Industrial Security of a task force effort to develop a handbook for security problems, but this product is not yet published(2:18).

There are several different definitions of security as well as different kinds of security. For the most part, in this paper, the kind of security talked about is data security. Data security protects against accidental or unauthorized loss, modification, use, or disclosure of data(2:26). It makes little difference in the end result whether data destroyed or modified was done accidentally or intentionally if such action was unwanted. Some definitions confine security to the protection of classified defense information and apply privacy to commercial or industrial sensitive information(3:38). This appears to be an unnecessary complication since industry is involved with defense information and data security as defined above can provide protection to both kinds of data. Further, making such a restrictive definition of privacy causes confusion with the issue of personal privacy which has been much in the news of late as a result of the expanding use of the computer by credit bureaus and government agencies(4).

In this paper security measures will be examined in three areas: (1) in the computer, (2) in the computer facility, and (3) external to the computer facility. The security measures to be taken in these three areas are interrelated. There are generally four requirements for good security: identification, authorization, audit, and system integrity(2:28). These requirements will be discussed as they pertain to each of the three areas. Since security is generally a more difficult problem in multi-programming or time-sharing use than in batch processing, only the former will be considered. Many of the measures are equally applicable to the latter method of operating a computer system.

Within the computer, both hardware and software features can be used to satisfy the identification requirement. It is usually necessary to know who is accessing the computer particularly with remote terminals. If the remote terminal

is within the company and is connected to the computer with special single use lines, the identification of the terminal can be accomplished through hardware features. IBM has developed a system for unique identification of any remote terminal through characters generated only by electronic circuitry(2:28). Identifying the operator of the terminal is a more difficult matter. Many systems use passwords but they provide little security. Other systems use what is known as extended handshaking, i.e. putting questions in the computer only the particular user knows how to correctly answer. The main objection to this method is the cost in time and memory space. A proposed method not yet perfected is fingerprint readers or voice print recognition. Perhaps the system with the most promise is a card the size of a credit card with a magnetic stripe containing identification characters. The card can be lost but the finder would have to know what the owner of the card was authorized to do to make use of the card.

The authorization function is usually handled within the computer by software features. The monitor is the key to a secure system. It must control all input/output without exception. It acts as the overall guard of the system, operating under a set of rules by which it judges all requested actions(5). An example of the various levels of authorization is shown in TRW's Generalized Information Management System. In this system there are three levels of data at which security can be imposed: system, data list, and attribute(6:21). The monitor imposes security codes as required at each of these levels for two reasons: functional protection and data sensitivity. While a particular group of individuals may require access to certain files, it is usually not desirable to permit all of them to update the data. Those authorized to update data have a special code. In the same way, there is certain data such as employee salary and future product design which is limited to particular individuals by the same kind of code system.

Approved For Release 2004/02/10 : CIA-RDP79M00096A000100070008-1

The computer is well adapted to satisfying the third security requirement, audit. It can maintain a continuing log of what went on, e.g. who accessed what file, and can sound an alarm when something not allowed is happening(2:30). The log is the ultimate defense against penetration as it provides the feedback necessary to strike the right balance between desired level of confidence and the impairment of production of the system due to interference of security restrictions.

The fourth requirement is system integrity. What is the probability that the computer will malfunction or make an error? Stated another way, what is the predictability of the system doing what you want it to do? There are several ways to obtain quality assurance, depending on what confidence level is desired and what cost is acceptable. For example, the control unit accesses one of the devices attached to the computer. What is the probability that this is the right device? If that probability does not give the required confidence level, it can be improved by programming another check in series with the device selection. The system can provide for identification of the data contained on the device. In this case the overall probability of having the system operate on wrong data as though it were the correct data is the product of the probabilities of the two individual errors. This results in a very low probability and a high confidence level. Another way to improve integrity is to thoroughly test and debug the program. Perhaps no program can be completely error free but with proper testing it can be nearly so. The coding in the monitor program which receives interrupts is one portion that must be error free. The confidence level can be improved by providing test programs in the monitor which routinely "attack" the system and try to break through the security barriers(7:3). Debugging or program testing presents special problems. An error in a program should not be able to destroy some other program or core memory nor should an error result in the same procedures as is employed on an

Approved For Release 2004/02/10 : CIA-RDP79M00096A000100070008-1 suspension

of the offending program. The security rules cannot be suspended for a debugging operation. The usual approach is to flag that a debugging operation is in progress. Then, if a violation occurs, it is logged and the program is dumped to the user with the reason. This avoids sounding a major security alarm for an error during a debugging operation.

What would seem to be the most obvious security precaution in the computer facility is to keep unauthorized personnel out of the facility. However, many companies maintain their computer facilities as show places and give relatively little supervision to visitors. These companies have given no thought to the serious damage that could result from such a policy. For example, one person with a magnet in his pocket could cause havoc in the tape library. Letting in only those with business in the computer facility satisfies the identification requirement.

In the same way that individuals are identified, each should be authorized to do only certain things. Certainly the number of operating personnel who are authorized to make changes to programs or internally stored data should be strictly limited. The reasons for this are obvious when the serious consequences of even a minor change are considered. In a case at Cape Kennedy, a computer symbol equivalent to a comma was omitted from a program causing a missile to veer so far off course it had to be destroyed(8:124). The personnel in a computer facility should comply with the operating procedures provided. From this it follows that there should be complete, current, and understandable instructions for all machine operation. One final item under the authorization requirement is designation of which individuals should have access to what type of classified or sensitive information. This requires that information of that type such as data relating to customer credit, shareholders, and payroll, must be categorized by security levels. Operating personnel must be cleared to appropriate levels.

In the same way that a log is required within the machine to provide an audit trail, a log is required within the facility showing operator interventions, machine halts and other occurrences indicating unusual conditions as well as machine performance in general, maintenance periods and compliance with operating schedules. The library is another area of great importance to the audit requirement. In addition to establishing controls over the use of library tapes, complete records of such use should be maintained. Procedures for maintaining libraries should include the requirement for backup tapes of current operating programs on data files. Such tapes can be invaluable in restoring lost or damaged data in case of a casualty or disaster to the computer itself.

While many companies are concerned about fraud through use of computers, a much greater danger is presented by inadvertent error. In the present state of the art of ADP the system integrity is highly dependent on human frailty. Humans make errors and every possible way must be taken to reduce such error to the lowest possible level. One way is to establish a quality control unit to sample the accuracy of data both before and after computer processing. This unit's function should be to spot data that are obviously unrealistic and permit corrections before major trouble develops(8:123). The problem of selection, training, and measuring the performance of computer personnel must be given continuing attention. John Diebold contends that there is a general lack of standards in these areas and that computer personnel are becoming the major cost of ADP in the United States(9:16). This argues for much more attention to this important area. One fairly obvious measure that parallels keeping records of machine performance is the recording of personnel performance as a part of the records of the computer facility. This gives management a measure of how well each employee is doing as well as a means of spotting trouble areas and the need for extra training. System integrity will be improved if there are adequate plans for disruptions up to

major disasters. An obvious measure is protection against fire. In a recent instance, a light plane crashed into the building housing Applied Data Research, Inc., destroying the card files and some tapes. However, because the company had made a practice of storing all major source programs on Librarian tapes, they were able to recover from the disaster within a week(10:174). Duplicate or back up tapes of programs that are to be maintained should be stored in a location remote enough that they would not be likely to be lost in a disaster destroying the computer. Recovery from error is an important consideration. Data files that are maintained in core memory and are updated continuously must be dumped onto tape at frequent intervals if it is important to be able to recover quickly from an error or breakdown. However, this becomes quite expensive and a balance must be determined considering the likelihood of the need for recovery and the relative costs. Fortunately, hardware is becoming increasingly reliable reducing the need for recovery but such is not the case with software. It appears that software failures will be a problem for some time to come(11:31).

The final area in which security measures will be discussed is external to the computer facility. The problem of identification of remote terminals and users has already been discussed in connection with security measures within the computer. One possible measure not discussed was the fairly simple one of installing locks on the terminal. A different one for each user can be provided if necessary. The principal difficulty with this is the ease with which a lock can be overcome.

A principal consideration in connection with the authorization function is to determine the need for access to data by the personnel in the company. The more levels of access required and the more capability provided, the greater is the complexity of the system required. If a particular individual were to be permitted access to all the data on a particular file or files and none other the

problem of stating his authorization would be a simple one. In practice such simplicity seldom occurs. As files are combined to take full advantage of the capability of the data processing system, the authorization function becomes more difficult and complex. The need for access to data by personnel must be converted to a statement of authorization, what person is to see what data elements in what combinations and what values(2:30).

The audit function is most important to improve computer security. With the introduction of computers there was a lag in applying proper audit procedures to data processing operations because of the scarcity of auditors grounded in computer system principles. This condition is changing. The auditor must be involved from the inception of development of new computer systems. He should not have responsibility to develop a control system but rather to evaluate independently the procedures and facilities being designed to provide management an independent control appraisal of future systems. The auditor should make sure that computer systems are auditable when they become operational. In doing so he should use computer technology to the greatest degree possible. To some extent the audit work can then be performed as a by-product of regular computer operations. Among the techniques which can be used by the auditor are: (1) use of a model representing the company to test the accuracy of the system, (2) comparison or matching of two duplicate files, (3) sampling records on a random basis, (4) extracting specific records from the file, and (5) compilation of the results of a particular mathematical computation as a check on the accuracy of the application of the formula in a computer run. Any audit program should meet the requirements of certified public accountants, the Internal Revenue Service and Department of Defense auditors for companies involved in defense contracting(8:129).

System integrity might appear at first glance to be not dependent on anything external to the computer facility but it very definitely is. One way integ-

rity can be degraded is by wire tapping. This poses very definite problems for the wire tapper. If the system is well designed, the wire tapper will be unable to operate as an imposter terminal. He will only be able to listen with the hope that information of use to him will come along. One way to avoid even this loss of information to a wiretapper would be to use scramblers. However, this poses many problems when used with common carriers and the cost is generally too great to make it attractive. Another threat to integrity is eavesdropping. It is possible with relatively inexpensive equipment to eavesdrop on remote terminal devices. It is much more difficult to get anything worthwhile eavesdropping on a central computer complex. If the cost of eavesdropping is plotted as a function of distance, the cost increases quite rapidly as distance increases. This suggests the answer to the eavesdropping problem. The terminal devices should be designed so they do not radiate beyond an area that can be controlled for the particular application. Another item that comes under system integrity is insurance. It is best to avoid the loss but, if a disaster does strike such as fire, flood or vandalism, it is important to have enough insurance to cover the financial loss involved in reconstructing the programs and data files that were destroyed as well as the loss in revenue during the time required for the reconstruction. This is necessary even though a well maintained library of back up files is maintained. A final item is the establishment of an overall control philosophy. Some companies have eliminated traditional controls to check human calculations on introduction of computer systems because "computers don't make mistakes." Such a course is itself a mistake for computers are programmed and operated by humans. Assigning a top level executive the responsibility to direct corporate computer efforts is perhaps the most effective way to insure adoption of an up-to-date overall control philosophy.

In conclusion, two points should be made. The first is that 100% security is probably impossible. Good security depends on many different measures taken at different times and different places. These could be likened to the layers of an onion. One of them might be adequate to defeat a particular threat but all are necessary to provide a high level of confidence that all threats will be defeated. In any case, the level of security desired must be measured against the cost of obtaining it. The second concluding point is that good security depends on the entire organization whether there is an ADP system or not. Certainly, when the company has adopted an ADP system, all employees connected with the ADP system have a responsibility to ensure that data processing is adequately controlled and protected. But even those parts of the organization not directly connected with the ADP system should be included in the overall control philosophy. In the final analysis, the best security starts with top management and extends to all personnel.

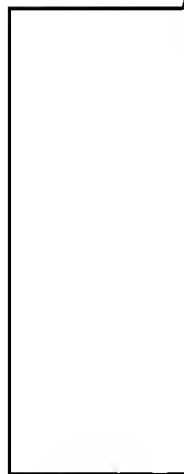
FOOTNOTES

1. This figure was stated by Dr. Carl Hammer on April 13, 1970 at the Industrial College of the Armed Forces.
2. _____ "Computer Security," transcript of the 15th Annual Seminar of ASIS. Industrial Security. December, 1969.
3. _____ "Problems and Potential Solution in Computer Control," transcript of the 14th Annual Seminar of ASIS. Industrial Security. April, 1969.
4. Richard I. Miller. "Computers and the Law of Privacy." Datamation. September, 1968.
5. Bernard Peters. "Security Considerations in a Multi-programmed Computer System." Paper delivered at Spring Joint Computer Conference, 1967.
- ✓ 6. _____ GLM System Summary, TFW Document No. 3181-A, 15 August, 1969.
7. Carl Hammer, Ph.D. "Security Considerations for Electronic Systems." Panel Presentation to Third National Seminar of National Classification Management Society, 1967.
8. Joseph J. Wasserman. "Plugging the Leaks in Computer Security." Harvard Business Review. September-October, 1969.
9. John Diebold. "Bad Decisions on Computer Use." Harvard Business Review. January-February, 1969.
10. _____ News Briefs. "Light Plane Lights ADR's Fire." Datamation. January, 1970.
11. Jan E. Hext. "Recovery from Error." Computers and Automation. April, 1967.

DATE JUN 18 JUN 1970

EXPIRES

STAT



500 (later)
23
19 June 70
P/S
525
[Signature]
[Signature]

RETURN TO:

FILE:

D E S T R O Y